
Audit of the Department's Efforts in Identifying IRM KSAs



FINAL AUDIT REPORT ED-OIG/A07-E0002 August 2004

Our mission is to promote the efficiency,
effectiveness, and integrity of the
Department's programs and operations.



U.S. Department of Education
Office of Inspector General
Kansas City, Missouri Office

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

In accordance with Freedom of Information Act (5 U.S. C. § 552) reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF INSPECTOR GENERAL

AUG 20 2004

MEMORANDUM

TO: William J. Leidinger,
Assistant Secretary for Management and Chief Information Officer

FROM: Helen Lew *Helen Lew*
Assistant Inspector General for Audit

SUBJECT: Final Audit Report - *Audit of the Department's Efforts in Identifying IRM KSAs*
Control No. ED-OIG/A07-E0002

Attached is the subject final audit report that covers the results of our review of the Department's efforts in identifying Information Resource Management (IRM) knowledge, skills, and abilities (KSAs) in accordance with the Clinger-Cohen Act. An electronic copy has been provided to your Audit Liaison Officer. We received your comments concurring with the finding and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS). ED policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the finding and recommendations contained in this final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after six months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during this review. If you have any questions, please call Richard J. Dowd, Regional Inspector General for Audit, at 312-886-6503.

Enclosure

600 INDEPENDENCE AVE., S.W. WASHINGTON, D.C. 20202-1510

Our mission is to ensure equal access to education and to promote educational excellence throughout the Nation.

Audit of the Department’s Efforts in Identifying IRM KSAs

Table of Contents

Executive Summary	1
Audit Results	2
Finding - The Department May not be in Full Compliance With the Clinger-Cohen Act Requirements for Developing IRM KSAs	2
Background	5
Objectives, Scope, and Methodology.....	6
Statement on Management Controls	7
Appendix I – Clinger-Cohen Core Competencies	
Appendix II – Auditee Comments	

Audit of the Department's Efforts in Identifying IRM KSAs

Executive Summary

The Department of Education (Department) has made progress in complying with the Clinger-Cohen Act¹ requirements for obtaining KSAs necessary to effectively perform IRM functions through limited workforce planning efforts. However, it did not use a systematic process in evaluating knowledge, skills, and abilities (KSAs); nor did it address the KSA requirements for all IRM staff. Without having identified the needed KSAs for all IRM staff, the Department was not able to develop a comprehensive strategy to eliminate deficiencies between needed and actual KSAs. As such, the Department's information resources management (IRM) may lack the basic KSAs needed to effectively manage information technology (IT) resources and investments; and to accomplish its goals. We recommend that the Department 1) use a systematic process such as the established core competencies in addressing the Clinger-Cohen requirements related to KSAs for IRM; and 2) ensure that skill assessments for the Office of the Chief Information Officer (OCIO) are tied to the IRM goals included in the Department's overall strategic plan.

We reviewed the Department's efforts to comply with the Clinger-Cohen Act requirements for obtaining KSAs necessary to effectively perform IRM functions. The objectives of our review were to determine the Department's progress in 1) identifying the KSAs needed for IRM; 2) developing a strategy to eliminate deficiencies between needed and actual KSAs; and 3) reporting progress made in improving IRM capability.

The Act requires federal agencies to determine the KSAs required for agency personnel in IRM and identify the current IRM staff qualifications; develop a strategy for narrowing the gap between the required KSAs and those of the current IRM staff; and report progress made in improving IRM capability. The Act also requires the Chief Information Officer (CIO) to assess the KSA requirements established for IRM personnel and ensure that those requirements link to IRM performance goals.

To assist federal agencies in complying with the requirements for assessing the IRM KSAs, the CIO Council developed the Clinger-Cohen Core Competencies to serve as a baseline for assessing KSAs. The established core competencies provide a systematic process and are endorsed by federal agencies. The Department did not use them in its KSA assessments for the OCIO workforce; nor has it used them in assessing whether the current requirements for its IRM workforce will enable it to meet its IRM performance goals. The Department also has not provided evidence that it used any specific guidance, criteria, or systematic process in its workforce planning efforts or that the future requirements for the IRM area have been coordinated with the Department's overall strategic plan.

OCIO concurred with our finding and recommendations. In addition, based on the Department's response that it is no longer considering a merger of OCIO with the Office of Management (OM), we eliminated the discussion of our concern about the Department's ability to maintain compliance with the Act given its plans to merge those two offices.

¹ Previously referred to as the Information Technology Management Reform Act of 1996, Division E of Public Law 104-106, 110 Stat. 679 (1996).

Audit of the Department's Efforts in Identifying IRM KSAs

Finding – The Department may not be Effectively Managing its IT Resources and Accomplishing Department Goals in Compliance With the Clinger-Cohen Act

The Department's workforce planning efforts have been limited – directed at identifying a strategy for replacing staff expected to retire in the next five years. However, the Department's planning efforts did not address the KSAs required for the remaining IRM staff. Further, the Department has not provided evidence that it used any specific guidance, criteria, or systematic process in its limited workforce planning efforts or that the future requirements for the IRM area are consistent with the Department's overall strategic plan. Without having identified the needed KSAs for all IRM staff, the Department was not able to develop a comprehensive strategy to eliminate deficiencies between needed and actual KSAs. Consequently, the Department may not be effectively managing its IT resources and accomplishing Department goals and, as a result, may not be in full compliance with Clinger-Cohen Act requirements.

The Clinger-Cohen Act requires federal agencies to determine the KSAs required for agency personnel in IRM and identify the current IRM staff qualifications; develop a gap analysis and strategy for eliminating differences between the required KSAs and those of the current IRM staff; and report progress made in improving IRM capability. The Act also requires the CIO to assess the KSA requirements established for agency personnel in IRM and the adequacy of these requirements for meeting IRM performance goals.

Specifically, the Clinger-Cohen Act (§ 5125(c)(3)) states that the CIO of an agency shall

annually, as part of the strategic planning and performance evaluation process...

(A) assess the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of such requirements for facilitating the achievement of the performance goals established for information resources management;

(B) assess the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements;

(C) in order to rectify any deficiency in meeting those requirements, develop strategies and specific plans for hiring, training, and professional development; and

(D) report to the head of the agency on the progress made in improving information resources management capability.

To assist federal agencies in complying with the requirements for assessing the IRM KSAs, the CIO Council developed the Clinger-Cohen Core Competencies to serve as a baseline for assessing KSAs. Although the core competencies give agencies a great deal of latitude in KSA assessments, they

provide a systematic process for deliberations in developing a set of KSAs needed in the IRM area. According to the CIO Council, using the core competencies allows CIOs to assess KSA requirements in compliance with the Clinger-Cohen Act. These core competencies have been endorsed by government agencies as members of the CIO Council, including the Office of Management and Budget (OMB), the U.S. General Accounting Office (GAO), and the Office of Personnel Management (OPM); and are used at the CIO University for training IRM personnel in federal agencies.

In addition to the Clinger-Cohen requirements, the President's Management Agenda includes requirements, under the Human Capital initiative, to assess knowledge and skills for staff. It requires agencies to assess the KSA requirements for personnel and determine their adequacy in achieving the performance goals established for agencies. According to GAO, the most important consideration in identifying skills and competencies is clearly linking them to an agency's mission and long-term goals. GAO stated that if an agency identifies staff needs without linking those needs to strategic goals, the needs assessment might be incomplete and premature.

The Department completed limited workforce-planning efforts, including planning for the IT workforce, and reported the results of its efforts in a Recruitment Plan. The Department's efforts focused on positions where possible retirements in the next five years could leave vacancies. The specific analyses performed included retirement eligibility, succession planning with a focus on supervisory and managerial positions, and an inventory of the skills and competencies needed by the workforce to successfully accomplish the Department's mission. Although the Department's plan identified a strategy for replacing staff expected to retire in the next five years, it did not evaluate the KSA needs for all IRM staff. Consequently, the Department's recruitment plan may not accurately reflect its needs and any actions taken by the Principal Offices may not meet the needs of both current and future workforce.

The Recruitment Plan stated that each Principal Office within the Department completed both a skills assessment and a skills gap analysis. However, without identifying the KSA needs for all IRM staff, the Department could not develop a comprehensive strategy to eliminate deficiencies between needed and actual KSAs. In addition, although the Department's Recruitment Plan identified the most critical positions within OCIO, OCIO provided no evidence that it performed any kind of assessment of the actual position requirements, including an assessment of whether those requirements assisted in meeting the IRM goals within the Department's Strategic Plan.

OCIO's assessment focused on how it would fill positions that might become vacant over the next five years due to employees retiring. OCIO developed a plan for closing the gap in KSAs created through expected, future retirements. The plan provided possible approaches for backfilling positions, including 1) whether qualified individuals exist in OCIO who could step into vacated positions; and 2) recruitment strategies for filling vacated positions through identifying employees elsewhere in the Department or through recruitment actions. Because the Recruitment Plan focused only on retirement planning, it did not address the KSAs required for the remaining IRM staff. As such, the Department's workforce planning efforts, to date, have been limited and do not fully comply with the Clinger-Cohen requirements for assessing IRM KSAs.

The Department's E-Government report to OMB provided information from the Department's Recruitment Plan. The Department also reported that it had developed specific training curriculum

to address identified deficiencies in the information security area; it would ensure that IT Project Managers have the skills necessary; and it would be tracking certifications of all IT Project Managers in the future. In addition, the report stated that the Department has developed a competency self-assessment tool that will assist in identifying individual competency development needs in the current workforce. This tool, known as the Employee Skills Inventory System (ESIS), is a voluntary, web-based electronic self-assessment tool that employees can use to identify competencies related to their jobs and assess their skills based on the competencies. Its E-Government report indicates the Department's willingness to address identified deficiencies. The Department's reported actions are in various stages of implementation, however, the effective implementation of all or any combination of the reported actions would not change our report findings.

According to the CIO Council, performing effectively in the established competency areas and possessing the knowledge, skills, and abilities under each competency area assists agencies in complying with KSA requirements in the Clinger-Cohen Act. Failure to use a systematic approach such as the established core competencies could result in the Department's failure to comply with the Act's requirements. More specifically, because it did not assess its entire IRM workforce against established competencies, the Department may not have effectively determined where important skill gaps are and how to efficiently and effectively address those gaps. As a result, the Department's information resource management may not have the basic core competencies or KSAs needed to effectively manage IT resources and investments. In addition, without a workforce plan that delineates the relationship between KSA requirements and the Department's IRM goals, the Department could have difficulty identifying current and future KSAs needed to accomplish its goals.

Recommendations

We recommend that the Assistant Secretary, Office of Management and Chief Information Officer

1. Use a systematic process such as the established core competencies in addressing the Clinger-Cohen Act requirements related to KSAs for all IRM staff;
2. Develop a comprehensive strategy to eliminate deficiencies between needed and actual KSAs; and
3. Ensure that skill assessments for OCIO are tied to the IRM performance goals included in the Department's overall strategic plan.

The Department's Comments and OIG Response

OCIO concurred with our finding and recommendations and provided a corrective action plan. Based on the Department's response that it is no longer considering a merger of OCIO with the Office of Management (OM), we eliminated the discussion of our concern about the Department's ability to maintain compliance with the Act given its plans to merge those two offices.

Audit of the Department's Efforts in Identifying IRM KSAs

Background

The Clinger-Cohen Act was enacted to address longstanding problems related to federal IT management. Among other things, it requires federal agencies to

- Determine the KSAs required for agency personnel in IRM;
- Determine the extent positions and personnel at executive and management level meet those requirements;
- Develop strategies for narrowing the gap between the required KSAs and those of the current IRM staff, including specific plans for hiring, training, and professional development for any identified deficiency; and
- Report progress made in improving IRM capability.

OMB, GAO, and OPM provide guidance for implementing the Clinger-Cohen Act, including requirements for obtaining and retaining the necessary KSA's for IRM. This guidance defines what an agency would need to accomplish in order to comply with the Act. In addition, the CIO Council developed a set of core competencies to assist agencies in complying with the Clinger-Cohen Act's requirements for assessing KSAs in the IRM area. The established core competencies are organized into 12 areas with detailed core competencies or KSAs under each area. These areas include Leadership/Managerial, Project/Program Management, Information Resources Strategy and Planning, Enterprise Architecture, Capital Planning and Investment Assessment, and IT security/information assurance. For a complete list of the 12 areas and the core competencies associated with each see the Appendix.

Audit of the Department's Efforts in Identifying IRM KSAs

Objectives, Scope, and Methodology

The objectives of our audit were to determine the Department's progress in 1) identifying the KSAs needed for IRM; 2) developing a strategy to eliminate deficiencies between needed and actual KSAs; and 3) reporting progress made in improving IRM capability. We did not assess the KSAs for OCIO organizationally nor did we assess KSAs of individuals within the Department's IRM area.

To accomplish our objective, we reviewed applicable policies and procedures, as well as laws, regulations, and agency guidelines. We interviewed officials in the CIO's office, including the CIO, to obtain information on the Department's goals, strategies, and staffing plans. We obtained and reviewed the Department's strategic plan, including the IRM section on strategic planning and workforce analyses; and strategic program planning documents, including the plan that guided staffing and the annual staffing plan. To meet our objectives, we did not use electronic data from the Department.

To assist in assessing the Department's efforts, we reviewed GAO reports on human capital and workforce planning at other federal agencies. We also reviewed human capital literature-including OPM's Human Capital Assessment and Accountability Framework as well as workforce planning models at OPM, OMB, and GAO.

We conducted work at the Department's CIO offices in Washington, D.C. and our OIG office in Kansas City, MO, during the period October 2003 to April 2004. We held an exit conference with Department officials on June 15, 2004. Our audit was performed in accordance with generally accepted government auditing standards appropriate to the scope of the review.

Audit of the Department's Efforts in Identifying IRM KSAs

Statement on Management Controls

As part of our review, we gained an understanding of the Department's management control structure applicable to the scope of the review. For purposes of this review, we assessed and classified the significant management controls related to the Department's IT efforts into the planning and assessment activities over the Department's IRM capabilities. The assessment also included a determination of whether the processes used by the Department provided a reasonable level of assurance of compliance with the Clinger-Cohen Act.

Because of inherent limitations, and the limited nature of our review, a study and evaluation made for the limited purpose described above would not necessarily disclose material weaknesses in the management control structure. However, our assessment identified a weakness in the Department's efforts to identify the KSAs needed for its IRM as set out in the *Findings* section of this report.

Audit of the Department's Efforts in Identifying IRM KSAs

Appendix I -- Clinger-Cohen Core Competencies (Revised June 2003)

The Clinger-Cohen Core Competencies, developed by the CIO Council, have been endorsed to serve as a baseline to assist government agencies in complying with Section 5125(C)(3) of the Clinger-Cohen Act. To perform effectively in each competency area below, an organization should possess the knowledge, skills, and abilities in each competency.

1.0 Policy and Organizational

1.1 Department/Agency missions, organization, functions, policies, procedures
1.2 Governing laws and regulations (e.g., the Clinger-Cohen Act, E-Government Act, GPRA, PRA, GPEA, OMB Circulars A-11 and A-130, PDD 63)
1.3 Federal government decision-making, policy making process and budget formulation and execution process
1.4 Linkages and interrelationships among Agency Heads, COO, CIO, and CFO functions
1.5 Intergovernmental programs, policies, and processes
1.6 Privacy and security
1.7 Information management

2.0 Leadership/Managerial

2.1 Defining roles, skill sets, and responsibilities of Senior Officials, CIO staff and stakeholders
2.2 Methods for building federal IT management and technical staff expertise
2.3 Competency testing - standards, certification, and performance assessment
2.4 Partnership/team-building techniques
2.5 Personnel performance management techniques
2.6 Principles and practices of knowledge management
2.7 Practices which attract and retain qualified IT personnel

3.0 Process/Change Management

3.1 Techniques/models of organizational development and change
3.2 Techniques and models of process management and control
3.3 Modeling and simulation tools and methods
3.4 Quality improvement models and methods
3.5 Business process redesign/reengineering models and methods

4.0 Information Resources Strategy and Planning

4.1 IT baseline assessment analysis
4.2 Interdepartmental, inter-agency IT functional analysis
4.3 IT planning methodologies
4.4 Contingency planning
4.5 Monitoring and evaluation methods and techniques

5.0 IT Performance Assessment: Models and Methods

5.1 GPRA and IT: Measuring the business value of IT, and customer satisfaction
5.2 Monitoring and measuring new system development: When and how to "pull the plug" on systems
5.3 Measuring IT success: practical and impractical approaches
5.4 Processes and tools for creating, administering, and analyzing survey questionnaires
5.5 Techniques for defining and selecting effective performance measures
5.6 Examples of, and criteria for, performance evaluation
5.7 Managing IT reviews and oversight processes

6.0 Project/Program Management

6.1 Project scope/requirements management
6.2 Project integration management
6.3 Project time/cost/performance management
6.4 Project quality management
6.5 Project risk management
6.6 Project procurement management
6.7 System life cycle management
6.8 Software development

7.0 Capital Planning and Investment Assessment

7.1 Best practices
7.2 Cost benefit, economic, and risk analysis
7.3 Risk management-models and methods
7.4 Weighing benefits of alternative IT investments
7.5 Capital investment analysis-models and methods
7.6 Business case analysis
7.7 Integrating performance with mission and budget process
7.8 Investment review process
7.9 Intergovernmental, Federal, State, and Local Projects

8.0 Acquisition

8.1 Alternative functional approaches (necessity, government, IT) analysis
8.2 Alternative acquisition models
8.3 Streamlined acquisition methodologies
8.4 Post-award IT contract management models and methods, including past performance evaluation
8.5 IT acquisition best practices

9.0 E-Government/Electronic Business/Electronic Commerce

9.1 Strategic business issues & changes w/advent of E-Gov/EB/EC
9.2 Web development strategies
9.3 Industry standards and practices for communications
9.4 Channel issues (supply chains)
9.5 Dynamic pricing
9.6 Consumer/citizen information services
9.7 Social issues

10.0 IT security/information assurance

10.1 Fundamental principles and best practices in IA
10.2 Threats and vulnerabilities to IT systems
10.3 Legal and policy issues for management and end users
10.4 Sources for IT security assistance
10.5 Standard operating procedures for reacting to intrusions/misuse of federal IT systems

11.0 Enterprise Architecture

11.1 Enterprise architecture functions and governance
11.2 Key enterprise architecture concepts
11.3 Enterprise architecture development and maintenance
11.4 Use of enterprise architecture in IT investment decision making
11.5 Interpretation of enterprise architecture models and artifacts
11.6 Data management
11.7 Performance measurement for enterprise architecture

12.0 Technical

12.1 Emerging/developing technologies
12.2 Information delivery technology (internet, intranet, kiosks, etc.)
12.3 Desk Top Technology Tools

Source: Chief Information Officers Council

Appendix II – Auditee Comments on the Draft Report



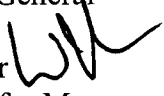
UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

ASSISTANT SECRETARY

July 16, 2004

TO: Richard J. Dowd
Action Regional Inspector General for Audit
Office of Inspector General

FROM: William J. Leiding 
Assistant Secretary for Management and Chief Information Officer

SUBJECT: DRAFT AUDIT REPORT – *Audit of the Department's Efforts in Identifying IRM KSAs* Control No. ED-OIG/A07-E0002

Thank you for your draft audit report, *Audit of the Department's Efforts in Identifying IRM KSAs*, Control No. ED-OIG/A07-E0002 sent June 4, 2004. The Office of the Chief Information Officer (OCIO) concurs with the single finding, "The Department may not be effectively managing its IT resources and accomplishing Department goals in compliance with the Clinger-Cohen Act." The following is our proposed corrective action to address the three recommendations your office has provided related to this finding.

Recommendation 1: Use a systematic process such as the established core competencies in addressing the Clinger Cohen Act requirements related to KSAs for all IRM staff.

Proposed Corrective Action: OCIO will work with the Office of Management Human Resources Services (HRS) to use the Clinger-Cohen core competencies developed by the CIO Council, and included as an Appendix in your draft audit report, to expand the core competencies for the IT Critical Occupation in Employee Skill Inventory System (ESIS). OCIO and HRS will develop and implement a strategy using ESIS to evaluate the actual and needed IT Knowledge, Skills and Abilities (KSAs) of Department staff based on these competencies.

Recommendation 2: Develop a comprehensive strategy to eliminate deficiencies between needed and actual KSAs.

Proposed Corrective Action: OCIO will work with HRS to develop a comprehensive strategy that addresses IT KSAs for new hires and existing staff. HRS staff have begun meeting with all hiring managers prior to the posting of vacancies to strengthen the recruitment process. OCIO and HRS will review existing EdHIREs IT questions to ensure that the full range of desired competencies are included to further strengthen IT recruitments. The IT KSAs will continue to be reviewed and emphasized when posting for IT positions. OCIO and HRS will develop learning tracks associated with the core competencies for the IT Critical Occupation to address the needed KSAs for existing staff.

Recommendation 3: Ensure that skill assessments for OCIO are tied to the IRM performance goals included in the Department's overall strategic plan.

Proposed Corrective Action: OCIO will work with the Strategic Accountability Service to add IRM performance goals to the Department's overall strategic plan.

Your draft audit report also included an "*Other Matters*" section that addressed a proposed reorganization of OCIO that would merge it with the Office of Management. This proposed merger is no longer being considered. Attached is the OCIO reorganization package that has received Department approval and is now being reviewed by the Union. The final proposal only includes internal restructuring.

Please contact Nina Aten on my staff if you have any questions. Ms. Aten can be reached on 202-401-5846.

Attachment



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

JUL - 9 2004

MEMORANDUM

TO: James Keenan, Director
Labor Relations Team

FROM: Darieta Cotton
Executive Office

SUBJECT: Reorganization of OCIO

The OM Executive Officer has approved the attached request to reorganize the Office of the Chief Information Officer.

Please arrange to notify the Union of this action if you believe that they should be notified. Your contact is Michell Clark who can be reached on (202) 260-7337.

Please let me know when and if the Union consultative meetings are scheduled.

Attachments

cc: Michell Clark



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

June 16, 2004

MEMORANDUM

To: Keith Berger, Executive Officer

From: William J. Leidinger

A handwritten signature in black ink, appearing to be "WL", is written over the name "William J. Leidinger".

Subject: Necessary Organizational Changes for the Office of the Chief Information Officer

This memorandum requests approval of a reorganization of the Office of Chief Information Officer (OCIO). This reorganization is intended to enhance OCIO's ability to serve the Department while better aligning the structure of the OCIO with the business needs of the Department. In addition, the reorganization establishes direct responsibility for those areas that require coordination on IT assets, policies and functions across the Department. The resulting OCIO organization will achieve these purposes:

- ✓ Better enables the accomplishment of the CIO responsibilities as outlined in the Government Information Security Reform Act (GISRA) and the Federal Information Security Management Act (FISMA).
- ✓ Aligns and prioritizes the information technology security policies, procedures and control functions under the CIO that are vested in the Chief Information Security Officer (CISO).
- ✓ Aligns the CISO directly under the CIO as required under GISRA and FISMA.
- ✓ Provides a central focus for training and overseeing personnel with significant information technology security responsibilities.
- ✓ Enhances the coordination and execution of the critical infrastructure protection responsibilities vested in the Department's Critical Infrastructure Officer (CIAO) as required in Presidential Decision Directive (PDD) 63. PDD 63 provides a framework for protecting critical infrastructure, which is generally referred to as those physical and cyber based systems essential to the minimum operations of the economy and government. The directive requires every department and agency to appoint a CIO who shall be responsible for the protection of its critical infrastructure.

The specific changes proposed are as follows:

- Move the Development Services Group from Information Management to Information Technology Operations and Maintenance Services. This will enable the Development Services Group, which develops, maintains and updates the department's web sites, to be part of, and integrated with, the group that it works most closely with and which supports and operates the Department's web sites.
- Move the information collection, FOIA, the Government Paperwork Elimination Act and records management functions from Information Management to the new Regulatory and Information Management Services. The performance improvement of these functions is a high Department priority. These functions will receive more focus and attention, and closer supervision and direction than was possible when these functions were in Information Management.
- Move the enterprise architecture, data architecture, system development life cycle development process, and the business-technology interface functions from Information Management to an Enterprise Architecture Team in the new Business and Enterprise Integration Services.
- Move the Investment Management Group from Information Management to the new Business and Enterprise Integration Services.
- The co-locating of Enterprise Architecture and Investment and Acquisition Management as the components of Business and Enterprise Integration Services will effectively link the knowledge of the Department's business with the development and upgrading of the Department's enterprise architecture and its' ongoing IT investment planning and decision process.
- Eliminate the Information Management Group.
- Move the Information Assurance Group directly under the CIO. This will strengthen the Department's adherence to the requirements outlined in Clinger-Cohen as well as full integration and coordination of all security and critical infrastructure protection functions.

The OM Executive Office will formally service the Office of the Chief Information Officer. It has been doing so by agreement with the Chief Information Officer for the past year. The staffing of the Executive Office is unchanged and is not included in the staffing patterns.

Although there will be necessary personnel moves because of movement of functions, we are committed to assuring that there will be no adverse personnel impact on any OM or OCIO employees as a result of this reorganization.

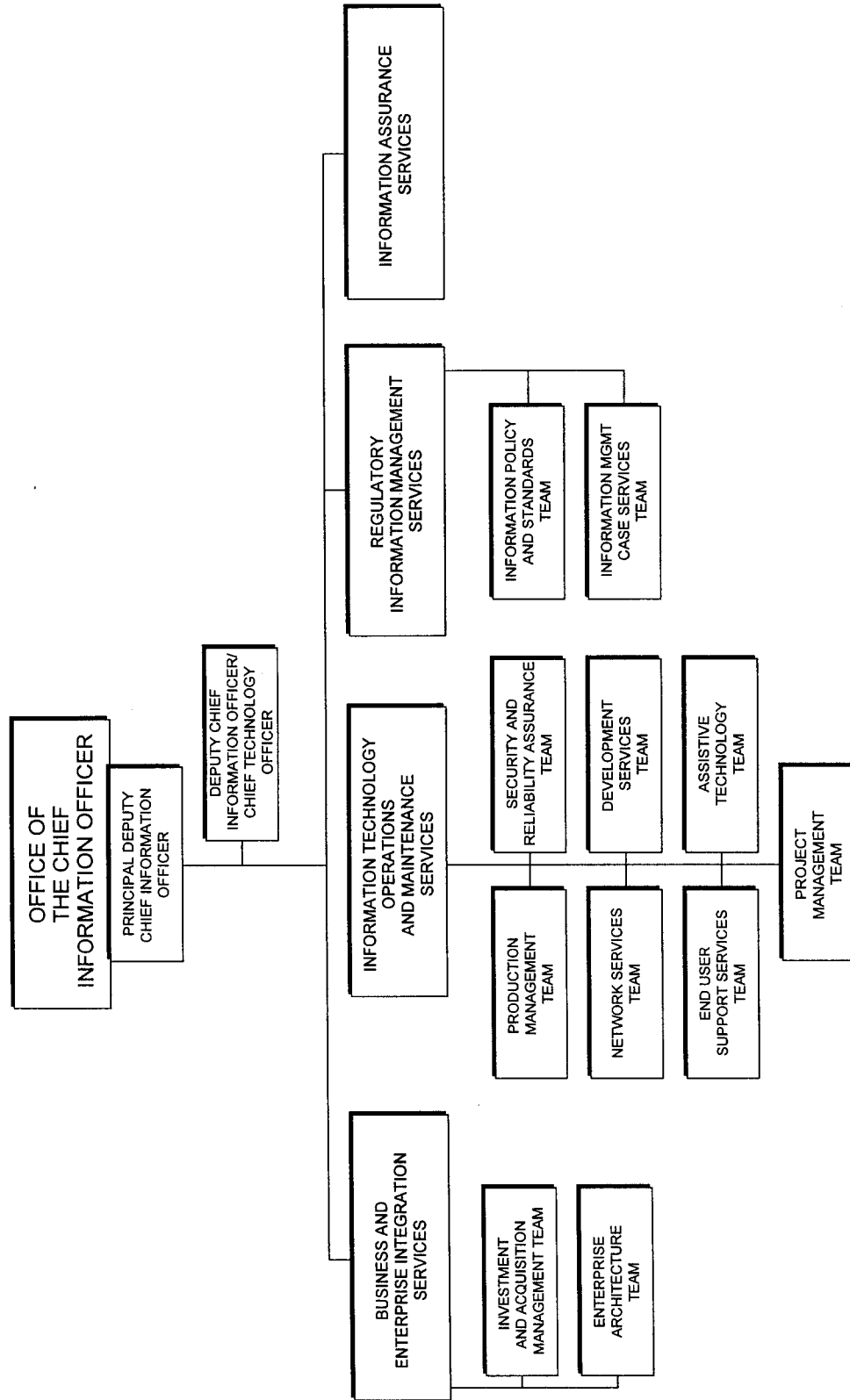
We will work with The Department's Delegations Control Officer to develop any necessary changes to existing delegations of authority that will be affected the reorganization.

Attachments:

- Tab A: Current Organization Chart
- Tab B: Proposed Organization Chart
- Tab C: Current Functional Statements
- Tab D: Proposed Functional Statements
- Tab E: Current Staffing Pattern for Affected Units
- Tab F: Proposed Staffing Pattern for Affected Units

TAB B

Proposed Organization Chart



TAB D

Proposed Functional Statements

OFFICE OF THE CHIEF INFORMATION OFFICER

SECTIONS

I. MISSION AND RESPONSIBILITIES

II. ORGANIZATION

III. ORDER OF SUCCESSION

IV. FUNCTIONS AND RESPONSIBILITIES OF THE OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO) COMPONENTS

A. IMMEDIATE OFFICE OF THE CHIEF INFORMATION OFFICER

B. INFORMATION MANAGEMENT

C. INFORMATION TECHNOLOGY

D. ENTERPRISE STRATEGY AND INFORMATION ASSURANCE

IV. PRIMARY DELEGATIONS OF AUTHORITY

I. MISSION AND RESPONSIBILITIES

The mission of the Office of the Chief Information Officer (OCIO) is to provide advice and assistance to the Secretary and other senior officers to ensure that information technology is acquired and information resources are managed for the Department in a manner that is consistent with the requirements of the Clinger-Cohen Act (40 U.S.C. 11315), the Paperwork Reduction Act of 1995 (44 U.S.C. chap. 35) and industry best practices. The agency's Chief Information Officer is charged with implementing the operative principles identified in the Act requiring the establishment of a management framework to improve the planning and control of information technology investments and leading change to improve the efficiency and effectiveness of agency operations.

The CIO reports directly to the Secretary and UnderSecretary and provides leadership and direction to:

- Develop, maintain, and facilitate the implementation of a sound and integrated information technology enterprise architecture;
- Promote the effective and efficient design and operation of major Departmental information resource management processes and recommend, as appropriate, improvements to agency business processes;
- Manage agency information resources to improve the productivity, efficiency, and effectiveness of Federal programs inclusive of information dissemination initiatives and efforts to reduce information collection burdens;

OFFICE OF THE CHIEF INFORMATION OFFICER

- Develop Information Technology (IT), Information Management (IM), and Information Assurance (IA) requirements, completing cost/benefit analysis of proposed solutions, managing projects in accordance with sound systems life cycle management procedures and establishing performance standards and measures to assess success of short and long term solutions;
- Define and manage IT, IM, and IA capital planning and investment management processes to ensure that they are successfully implemented and integrated with the Department's budget, acquisition and planning processes;
- Develop and submit recommendations to the Investment Review Board (IRB) regarding IT, IM, IA capital investments to assure that investment decisions are mission aligned, cost justified and approved only after careful and systematic review;
- Monitor the performance of the agency's IT, IM, and IA programs and investments, evaluating them against performance and other applicable measures, and advising the Secretary regarding their continuation, modification or termination;
- Assess IT, IM, and IA competencies defined for agency personnel to ensure that Departmental employees are technologically prepared to achieve the Department's strategic goals;
- Develop IT and IM requirements, analyze the projected cost and benefits of alternative IT and IM solutions, and establish performance standards and measures to assess short and long range solutions;
- Administer the Department's information resource management program, including records management, automated data processing activities, the Paperwork Reduction Act, Government Paperwork Elimination Act, Freedom of Information Act, Privacy Act, and the Information Quality Guidelines;
- Manage the agency's IT Security Program for automated information systems, developing agency-wide policy for the protection and control of information resources directly or indirectly related to the activities of the Department;
- Implement a Department-wide communications Internet/Intranet strategy;
- Deploy and maintain all enterprise-wide information technology;
- Develop recommendations and implement information technology solutions designed to enhance and enable agency business processes;
- Develop and provide technology standards to assure business alignment and promote a viable enterprise technology framework;

OFFICE OF THE CHIEF INFORMATION OFFICER

- Provide administrative and technical support to the agency's Data Integrity Board and monitor the Department's compliance with the Computer Matching and Privacy Protection Act.

II. ORGANIZATION

The Office of the Chief Information Officer (OCIO) is under the immediate supervision of the Chief Information Officer (CIO). In carrying out the responsibilities of the Department described in 44 U.S.C. 3506, 40 U.S.C. 11315(b) and (c), and Executive Order 13011, the Chief Information Officer reports directly to the Secretary and Under Secretary.

III. ORDER OF SUCCESSION

The Order of Succession for the Office of the Chief Information Officer is as follows:

Principal Deputy Chief Information Officer
Deputy Chief Information Officer/Chief Technology Officer
Director, Information Technology
Director, Information Management.

OFFICE OF THE CHIEF INFORMATION OFFICER

IV. FUNCTIONS AND RESPONSIBILITIES OF OCIO COMPONENTS

A. THE CHIEF INFORMATION OFFICER

The Chief Information Officer (CIO) provides advice and other assistance to the Secretary and Under Secretary in information technology (IT) matters and other IT activities and functions as directed. The CIO is responsible for developing and maintaining a sound and integrated IT architecture for the Department while also promoting the efficient design and operation of all major information resources processes for the agency. The CIO provides strategic leadership and executive direction to the office's organizational components to ensure successful accomplishment of the office's mission. The CIO manages the agency's relationship to Federal CIO Council Initiatives and coordinates Council activities throughout the Department.

The Principal Deputy Chief Information Officer (PD CIO) serves as the alter ego for and supports the CIO in IT matters and other activities and functions as directed. The PD CIO assists the CIO by providing day-to-day operational priorities, strategic leadership and executive direction to the Office's organizational components to ensure successful accomplishment of the Office's mission. The PD CIO performs administrative duties such as performance evaluations for the Deputy CIO/CTO and other senior leadership within the Office. The PD CIO provides advice to the Secretary, other Senior Officers and the CIO, and promotes the effective and efficient design and operation of all major information resources processes for the Department.

The Deputy Chief Information Officer/Chief Technology Officer (CTO) assists the CIO in the development of standards, guidelines, and policies to transform current ED data collection and information management processes. The CTO advises the ASM/CIO and PD CIO on new and emerging technologies in the areas of communication, information technology, and IT system development that may benefit the Department. The CTO supervises the operation of Business and Enterprise Integration Services.

B. INFORMATION TECHNOLOGY OPERATIONS AND MAINTENANCE SERVICES

Information Technology Operations and Maintenance Services supports the CIO's efforts in all activities related to network information enterprise, to include network security, network and telecommunications design and operations, end user services, production server hosting services, and ED's intranet and Internet services as well as maintains and operates ED's disaster recovery facility.

The Office is headed by a Director who reports to the Chief Information Officer. Information Technology Operations and Maintenance Services is divided into the following seven teams:

- Production Management Team;
- Network Services Team;
- End User Support Services Team;
- Security and Reliability Assurance Team;

OFFICE OF THE CHIEF INFORMATION OFFICER

- Development Services Team.
- Assistive Technology Team; and
- Project Management Team

Production Management Team

The Production Management Team administers all servers that comprise EDNET which process all shared applications used throughout the Department.

In performing its responsibilities, the Team:

- Manages the daily operation and maintenance of all departmental servers that are hosted within EDNet.
- Provides scheduled backups, upgrades, and maintenance of EDNet hosted servers.
- Coordinates the overall operation of the Department's IT infrastructure.
- Recommends the Server Technology component of the enterprise architecture.
- Manages all mainframe, timesharing and related server services that offer centralized support to users Department-wide, including the Department's network.
- Designs and maintains the Department messaging services that allows it to quickly communicate with its employees, contractors, the citizenry, schools, municipalities, states, and researchers.

Network Services Team

The Network Services Team provides and maintains the infrastructure that allows individual Departmental end users to access shared applications that are hosted throughout the world from their local personal computers. Also, this Team maintains the telephone and video conferencing systems.

In performing its responsibilities, the Team:

- Orders and implements telecommunications services including local, long distance and dedicated services.
- Operates and maintains video telecommunications services for the Department.
- Administers the Network Control Center for the Department.

OFFICE OF THE CHIEF INFORMATION OFFICER

- Champions emerging collaborative technologies to make Department-wide users more effective in dealing with their peers and customers.
- Provides an access path for all End Users to be able to use IT infrastructure down to individual workstations, telephone handsets, IPTV displays, and video conferencing rooms.
- Manages the IT cabling plan.

End User Support Services Team

The End User Support Services Team ensures that all departmental employees regardless of their locations have appropriate access to the Department's services and that their personal computers work properly.

In performing its responsibilities, the Team:

- Manages the Help Desk, which is the entry point for virtually all requests for IT services.
- Provides work station on-site support.
- Manages and provides operational support for all office automation activities throughout the Department.
- Provides project management support for ED technology customers that are relocating offices.
- Oversees installation and disposal of workstation equipment.
- Provides operations support and serves as a liaison in the field for the Secretary's Regional Representatives (SRRs).
- Supports SRR implementation of agency-wide technology and applications solutions in the regional offices and provides ongoing customer and technical support.

Security and Reliability Assurance Team

The Security and Reliability Assurance Team protects the overall network from hostile attacks as well as manages a disaster recovery facility for all of the Department's critical applications. Also, the team ensures that all additions to hardware and software are adequately tested prior to their inclusion into EDNET.

In performing its responsibilities, the Team:

- Performs multi-tiered indepth defense against cyberterrorist attacks from viruses, worms, and hackers.

OFFICE OF THE CHIEF INFORMATION OFFICER

- Ensures reliable execution of all hosted servers through executing a production promotion process that test all updates to the production environment prior to implementation.
- Directs all activities related to the agency's alternate site for redundant systems as prescribed by the Department's system Disaster Recover Plans and Continuity of Operations Plan.
- Provides facility management support to the agency's alternate data processing center.
- Maintains portal security.
- Tests and evaluates all EDNet equipment.
- Provides administrative support to the Change Control Review Board.
- Develops and enforces processes and procedures to ensure sound configuration control and change management of EDNet and its tenant systems.

Development Services Team

The Development Services Team manages the web-based applications that support and enhance the agency's on-line business processes and provide additional application development support across the enterprise.

In performing its responsibilities, the Team:

- Develops and manages internet and intranet applications and coordinates the delivery of appropriate training for Departmental users.
- Enhances education information dissemination, develop new information resources and improve on-line business processes.
- Defines and explores opportunities for Government-to-Customer, Government-to-Business and Government-to-School e-business initiatives and measures effectiveness of new endeavors
- Maintains and operates ED's internet Web site, ed.gov.
- Maintains and operates ED's intranet Web site, connectED.
- Takes responsibility for putting content on the Web sites, including providing tools for adding Web site content.
- Works with Principal Offices on developing new content and updating existing content on the ed.gov and connectED Web sites.

OFFICE OF THE CHIEF INFORMATION OFFICER

Assistive Technology Team

The Assistive Technology Team evaluates and tests software applications and hardware to ensure compatibility with the legislative requirements of Section 508 of the Rehabilitation Act of 1973 (29 USC 794d) and the agency's operating environment.

In performing its responsibilities, the Team:

- Assists program offices with the evaluation, testing and implementation of assistive technology solutions for individuals with disabilities.
- Serves as liaison to schools and other federal agencies to facilitate the evaluation and implementation of assistive technology solutions in the classroom and the workplace.
- Provides advice to program offices regarding section 508 requirements for grant competitions.

Project Management Team

The Project Management Team ensures that all IT operation's projects are professionally managed and that IT delivers on its commitments.

In performing its responsibilities, the Team:

- Provides a core of qualified project managers that executes the OCIO's formal project management process in support of EDNET customers who require new solutions to be developed.
- Performs technology assessment and analysis.
- Provides administrative support to the Technology Review Board.
- Defines IT design elements and develops and tests solutions for emerging customer requirements.

C. BUSINESS AND ENTERPRISE INTEGRATION SERVICES

Business and Enterprise Integration Services (BEIS) provides leadership, oversight, and coordination of the Department's effort to ensure that its Information Technology (IT) investments support ED's strategic plan and are business driven. In particular, this relates to the following activities within the Department of Education:

- Capital Planning and Investment Control (CPIC);
- Enterprise Architecture development, usage and change management;
- Enterprise Architecture product quality and compliance measurement;
- Business Technology Interface;

OFFICE OF THE CHIEF INFORMATION OFFICER

- Systems Development Life Cycle; and
- IT Acquisition support.

BEIS is responsible for providing policies, standards, and procedures that ensure ED offices comply with the Department's investment review process and enterprise architecture. In addition, BEIS provides instruction to customers to help educate and support them in their investment review and enterprise architecture efforts.

The Deputy CIO/CTO is responsible for leadership, policy guidance, quality control, and coordination for Business & Enterprise Integration Services. The Deputy CIO/CTO also ensures that the operations of BEIS are consistent with federal laws and directives as well as Department standards, policies, and procedures. Furthermore, BEIS ensures that its operations are carried out in an effective and efficient manner, and are customer-oriented.

BIES is comprised of two Teams:

- Investment and Acquisition Management Team; and
- Enterprise Architecture Team.

Investment and Acquisition Management Team

The Investment and Acquisition Management Team is responsible for developing and implementing strategies and programs designed to enhance the Department's business case preparation and capital investment management and planning. The Team is also responsible for providing IT acquisition support to OCIO and the Department

In performing its responsibilities, the IT Investment Management Team:

- Develops and submits recommendations to the Investment Review Board (IRB) regarding IT investments (including projects, systems, IT workforce and initiatives) to assure that investment decisions are mission aligned, cost justified and approved only after careful and systematic review.
- Defines and manages IT investment management processes through a long-range planning and a disciplined budget decision making process to achieve performance goals and objectives with minimal risk, lowest life-cycle costs and greatest benefits for the agency. Ensures that the processes are successfully implemented and integrated with the Department's budget, performance-based acquisition and planning processes
- Oversees business case preparation for IT activities and services.
- Defines capital planning and investment policies and procedures so that the Department can best manage its resources and can measure and evaluate the benefits of investment decisions.

OFFICE OF THE CHIEF INFORMATION OFFICER

- Coordinates and supports investment decision processes across the agency that are prescribed by the Clinger-Cohen Act of 1996.
- Coordinates activities with the OCIO and across offices that link mission needs and capital assets in an effective and efficient manner.
- Develops and promotes Department-wide IT investment performance measures to assess agency progress in meeting requirements under the Government Performance and Results Act, the Information Technology Reform Act, and other relevant legislation.
- Administers and provides oversight for procurement and contract management of IT activities, and provides acquisition support to IT staff.
- Facilitates Department IT acquisition activities and manages the office's relationships with vendors and other OCIO contractors.
- Manages Department-wide software and system licenses, including procurement, test, and implementation phases.

Enterprise Architecture Team

The Enterprise Architecture Team is responsible for capturing the description of how the Department does its business, and what information, data, and technology are required to support the business. Furthermore, the Enterprise Architecture Team is responsible for the Department's system development life cycle and the business technology interface. The Team also includes Business Technology Advisors who provide direct coordination services between OCIO and the Principal Offices.

In performing its responsibilities, the Enterprise Architecture Team:

- Develops, maintains, and facilitates the implementation of a sound and integrated IT enterprise architecture.
- Provides written organizational policy, for approval by the Executive Management Team and the Investment Review Board, regarding the governance of the enterprise architecture.
- Uses the enterprise architecture to analyze IT solutions and ensure that they support the business of the Department.
- Leverages methodologies to eliminate redundancies, reduce cost, and manage change.
- Provides Business Technology Interface support to document requirements for, analyze, and justify each business case presented to the Investment Review Board.

OFFICE OF THE CHIEF INFORMATION OFFICER

- Uses the enterprise architecture to analyze deliverables proposed by Principal Offices to ensure the statements of work are complete, as outlined in the Systems Development Life Cycle (SDLC).
- Monitors and provides reviews for enterprise (information, data, systems, and technology) within the SDLC, CPIC, and acquisition processes.
- Ensures enterprise architecture products are identified, tracked, monitored, documented, reported, and audited.
- Manages and provides enterprise architecture repository maintenance, oversight, training, and version control.
- Ensures enterprise architecture products and supporting processes are prepared to undergo an independent verification and validation.
- Applies metrics for measuring enterprise architecture progress, quality, compliance, in order to calculate the return on investment.

D. Regulatory Information Management Services

Regulatory and Information Management Services (RIMS) provides leadership, oversight, and coordination to ensure Departmental compliance with government initiatives regarding the acquisition, release and maintenance of information. In particular, this relates to the following activities within the Department of Education:

- Freedom of Information Act (FOIA);
- Privacy Act;
- Records Retention and Management;
- Information Collection;
- Government Paperwork Elimination Act (GPEA); and
- Information Quality Guidelines (IQG).

RIMS is responsible for providing policies, standards, and procedures that ensure ED complies with governmental information management requirements in the above areas. In addition, RIMS provides instruction to assure that customers are educated and supported in the performance of these efforts.

The office is headed by a Director who reports to the Chief Information Officer. RIMS includes two teams:

- Information Policy and Standards Team; and
- Information Management Case Services Team.

OFFICE OF THE CHIEF INFORMATION OFFICER

The office of the Director includes a Special Assistant for Appeals Services who is responsible for the oversight, coordination and disposition of all agency appeals regarding the Freedom of Information Act (FOIA) and the Department's IQGs.

Information Policy and Standards Team

The Information Policy and Standards Team is responsible for developing and implementing strategies and programs designed to enhance the Department's responsiveness to government information management requirements regarding the acquisition, release and maintenance of information.

In performing its responsibilities, the Information Policy and Standards Team:

- Promotes the effective and efficient design and operation of major ED information resource management processes; and, as appropriate, examines and recommends improvements to agency business processes.
- Supports the policies and procedures of management, analysis and protection of federal, state, and local data collected and disseminated by the Department.
- Articulates standards for the Department's IQG's, and provides guidance and technical assistance to program offices on quality, dissemination, privacy, and security issues.
- Issues directives and handbooks to support and enhance the performance of agency responsiveness to information management initiatives.
- Provides instruction designed to help agency personnel better coordinate intra- and inter-agency efforts regarding the acquisition, release and maintenance of information.
- Supports agency information to improve the productivity, efficiency, and effectiveness of federal programs including information dissemination initiatives and efforts to reduce information collection burdens.
- Champions e-records management and works to ensure that enterprise-wide e-records policies are adopted.
- Works with client offices to plan for and coordinate enterprise-wide information access, data collection and records management activities.
- Manages the implementation of the Government Paperwork Elimination Act (GPEA) across the agency.
- Provides leadership and coordination in the resolution of sensitive and high-risk information management cases.

OFFICE OF THE CHIEF INFORMATION OFFICER

Information Management Case Services Team

The Information Management Case Services Team is responsible for the comprehensive operation of the agency case management system that responds to FOIA and Privacy Act requests. The Team also is responsible for supporting ED information collection, records retention and management, and GPRA activities.

In performing its responsibilities, the Team:

- Oversees agency compliance with FOIA, Privacy Act and Departmental records retention and management policies.
- Ensures the successful handling of all requests regarding FOIA and the Privacy Act received by the Department. The team also is responsible for furnishing reliable, accurate, and timely information on FOIA and the Privacy Act in compliance with relevant laws, statutes, regulations and directives.
- Administers the agency's information collection activities, overseeing the Department's collection and reporting processes under the Paperwork Reduction Act and preparing the annual Information Collection Budget for transmittal to OMB.
- Supports Department systems and databases associated with information collections, FOIA, Privacy, and records retention and management.
- Oversees and monitors the administration of contracts to support operation and maintenance of systems and databases relating to the mission of RIMS.

E. Information Assurance Services

Information Assurance Services oversees the Department's IT security program and implementation of the Federal Information Security Management Act. The Director of Information Services reports directly to the Chief Information Officer.

In performing its responsibilities, the Information Assurance Team:

- Directs the Department's enterprise-wide information assurance activities, developing policies and guidance to prevent and defend against unauthorized access to networks, system, and data directly or indirectly related to the Department's activities.
- Provides agency-wide leadership in maintaining and improving the accuracy, confidentiality and integrity of data maintained in the Department's information systems, including ongoing support of the agency's Data Integrity Board and data matching/exchange agreements with other agencies.

OFFICE OF THE CHIEF INFORMATION OFFICER

- Coordinates agency-wide IT security incident reporting and emergency response activities and serves as the Department liaison with the Office of General Counsel, Fed CIRC, the FBI, and other external law enforcement agencies concerning IT security incident reporting and follow-up activities.
- Implements and coordinates activities regarding the agency's Critical Infrastructure Protection (CIP) focusing on protecting mission essential infrastructure, promoting best practices in infrastructure management, and developing and promulgating policies to implement requirements of Presidential Direction (PDD) 63.
- Enforces Federal ADP Security standards, including review and evaluation activities prescribed by OMB Circulars A-123 and A-130.
- Coordinates agency-wide policies regarding authentication and message encryption techniques inclusive of digital signatures and PKI technology.
- Conducts annual Department-wide security audit reviews mandated by the Government Information Security Reform Act (GISRA) and periodically assists the agency's OIG with the conduct and resolution of Department IT security program and system audits.
- Manages the operation of the agency's Information and Critical Infrastructure Assurance Steering Committee.
- Develops and maintains a comprehensive and effective disaster recovery planning program that ensures continuity of operations for essential Departmental systems in the event of an emergency or other disruption to normal operations.
- Develops corrective action plans to address weaknesses disclosed by GISRA reviews, IG audits, and Federal Managers Financial Management Integrity Act (FMFESIA) annual certifications related to IT security matters.
- Defines IT security curricula and provides specialized security training for agency's technical staff and general security awareness/orientation training required of all Departmental employees.